Identity Theft by Christine Nelson

One of the fastest growing threats in today's electronic society is identity theft. Our vulnerability to cyber identity theft has never been higher. The larger data security breaches such as Target, Sony and Morgan Stanley get a lot of press but every minute there are hackers successfully taking personal financial or identity information and turning it into a profitable cyber black market. Use of ATMs, credit and debit card readers and our ever present smart phones and tablets make the opportunities for electronic identity theft even more promising. A more recent threat is in the form of individuals stealing social security numbers and filing fraudulent tax returns with a change of address to receive refunds. The actual tax payer is usually not discovering this theft until the IRS notifies them that their return has already been filed. It could be several weeks after the crime was committed before the issue is identified.

The regulatory arena is attempting to keep up with this increased threat and is requiring companies to implement stiffer technology controls and cybersecurity processes in an effort to reduce the spread of electronic fraud. In addition, there is a significant priority to verify customers' identities as they request activity in their accounts.

In 2013 the SEC and CFTC Regulation S-ID program became effective requiring financial institutions to have a written identity theft prevention program designed to limit client exposure to potential fraud in their accounts. In summary, the program requires financial institutions to have safeguards and training in place to detect suspicious activity or "red flags" in client accounts, particularly with requests for money transfers or changes of address. Requests for funds or changes of address by email, text or even phone calls should be confirmed through a signed letter, an in-person exchange and/or a series of security questions confirming that it is indeed the client requesting the activity.

This type of regulation will probably only increase as the cybersecurity arena gets more complex and hackers become more adept at accessing our personal credentials. Cyberattacks have no geographic borders so countries all over the world are facing this heightened level of fraudulent activity.

These days individuals are required to be vigilant in their protection of personal credentials and identity. The era of locked filing cabinets is changing and we have to increase our awareness of the potential for theft in our electronic lifestyle. Fraudulent activity is becoming easier as we all reach for our devices on a more frequent basis.

What can you do to reduce your risk of identity theft or fraud?

- Keep your personal information personal. Do not keep important credentials on your smart phone or your tablet or at least make sure they are in a password protected location
- Create passwords (or other access barriers like thumbprints) for your smart phone, computer, laptops and tablets and change them frequently. Do not make passwords all the same or even similar.
- Do not create an easily accessible list of these passwords. There are good apps for storage requiring levels of authentication
- Do not allow browsers to store your passwords for financial websites. Although convenient, it is an absolute open door invitation for a thief who has found or stolen or even cloned your device from across the room
- Be careful when using unsecured Wi-Fi. Public Wi-Fi access is a great way to let hackers access anything you may be browsing or have stored on your personal device whether smart phone, tablet or laptop
- Be very wary of phishing emails. Hackers are ever more crafty masquerading emails with well-known logos of trusted companies to trick you into opening an email on your device embedded with malware. If you aren't expecting information from that vendor or solicitor, do not open the email. You can call the company to determine the validity of the email.
- Install personal firewalls on your computers and malware and virus protection on your devices. This is a first line of defense for many intruding viruses and malware which can take over your devices and personal information
- Do not send important credentials like your social security number or financial account numbers through an unencrypted email or text. If you must share this information, call the recipient directly (confirming you have reached the desired institution) and give the information.
- If your financial advisor, banker or broker does not have this policy in place already, ask them to call you directly and confirm any wire or money transfer requests or a change of address request they may receive by email. Hackers can easily replicate former requests including familiar salutations and account information if they have accessed your email account.
- Create online access to your financial accounts and credit cards and then check activity daily. This is the fastest way to recognize suspicious or fraudulent activity in your accounts. Consider it as much as a 30 day head start on catching fraudulent activity instead of waiting for your paper statements in the mail. These sites are usually good at requiring multiple authenticators for security purposes. (Again, do not allow financial websites in particular to store your password information.)
- Check your credit reports at least annually to confirm there are no unauthorized credit accounts or debts in your name.
- Sign up for one of the credit and identity theft monitoring programs. Do research on the level of monitoring you desire.

Altavista Wealth Management, Inc.

4 Vanderbilt Park Drive
Suite 310
Asheville, NC 28803
Phone (828) 684-2600
Fax (828) 684-2680

6525 Morrison Boulevard
Suite 107
Charlotte, NC 28211
Phone (704) 365-4867
Fax (704) 365-4868

Altavista Advisors

L. Daniel Akers, Jr., *CFP®, CPA*
Managing Principal

Kyle R. Boyd
Managing Principal

Jacqui S. Friedrich, *CFP®*
Financial Advisor, Director of Financial Planning

W. Edmond Zorigian
President, Altavista Trust